UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/596,009	06/16/2000	Brig Barnum Elliott	00-4010	2514

32127 7590 12/02/2004

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQEO3H14
IRVING, TX 75038

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/596,009	ELLIOTT, BRIG BARNUM	
	Examiner	Art Unit	
	Aravind K Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/12/04*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 are pending in the application.

2. Claims 1-36 have been rejected.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/12/04 has been entered.

Response to Arguments

4. Applicant's arguments with respect to claims 1-36 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

5. Claims 1, 2, 6-8, 10-12, 15, 24-32 and 35 are rejected under 35 U.S.C. 102(e) as being anticipated by Rubino et al U.S. Patent No. 6,424,629 B1.

As to claims 1, 7 and 24, Rubino et al discloses a communications router for use in a communications network including a plurality of routers controlled by one or more trusted parties, and at least one network control computer communicating with the communications router, the communications router comprising:

a transceiver to transmit and receive messages [column 5 line 66 t column 6 line 17];

an electronic memory circuit having network information stored therein [column 15, lines 13-42];

an electronic processor circuit which (i) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning router of the plurality of routers and is to be excised from the network [column 8, lines 15-34]; (ii) determines an authenticity of the excising signal [column 8, lines 35-49]; (iii) excises the first router when the excising signal is authenticated [column 8, lines 50-58]]; (iv) reroutes the excising signal to at least a second router of the plurality of routers when the excising signal is authenticated [column 8, lines 59-65].

As to claims 2 and 8, Rubino et al discloses that the electronic processor circuit excises the first router by adding the first router to information regarding routers stored in the electronic memory circuit [column 15, lines 13-42]. Rubino et al discloses removing from the electronic memory circuit routing updates corresponding to the first router [column 15 line 52 to column 16 line 7]. Rubino et al discloses removing the first router from a neighbor table stored in the electronic memory circuit when the first router is listed therein [column 15 line 52 to column 16 line 7]. Rubino et al discloses recomputing a forwarding table to direct future routing [column 15 line 52 to column 16 line 7].

As to claim 6, Rubino et al discloses that the electronic processor reinstates the first router when the communications router receives and verifies a reinstate message from the network control computer [column 13, lines 47-63].

As to claims 10 and 11, Rubino et al discloses evaluating a signal received through the transceiver from another network router [column 8, lines 35-49]. Rubino et al discloses identifying which network router a signal has just been received from [column 7, lines 24-54]. Rubino et al discloses determining if the network router is identified by the information regarding excised routers [column 7, lines 24-54]. Rubino et al discloses discarding the signal when the router is listed [column 8, lines 50-58]. Rubino et al discloses processing the signal when the router is not listed [column 10, lines 15-31]. Rubino et al discloses processing the signal when the router is listed [column 10, lines 15-31]. Rubino et al discloses recomputing the forwarding table, as discussed above.

As to claim 12, Rubino et al discloses removing the second router from information stored in memory regarding routers controlled by trusted parties [column 11, lines 3-18]. Rubino

et al discloses removing from the communications router routing updates corresponding to the second router [column 15 line 52 to column 16 line 7]. Rubino et al discloses removing the second router from a neighbor table of the communications router when the second router is listed therein [column 15 line 52 to column 16 line 7]. Rubino et al discloses recomputing a forwarding table [column 15 line 52 to column 16 line 7].

As to claim 15, Rubino et al discloses the step of reinstating the second station when the communications router receives and verifies a reinstate message from the network control computer [column 16, lines 20-40].

As to claims 25 and 26, Rubino et al discloses in a communications system for communications among a plurality of routers in a network controlled by one or more trusted parties, at least on computer being linked to a first router of the plurality of routers, a method of operating the network comprising the steps of:

> authenticating in the first router a cut-off signal received from the control computer, the cut-off signal indicating that the control computer has determined that at least on functioning router is controlled by an untrusted party and is to cut-off from communicating with the network [column 8, lines 35-49];
>
> preventing the first router from communicating with the at least one cut-off router when the signal is authenticated [column 8, lines 59-65];
>
> redistributing the cut-off signal to each of the plurality of routers, except for the at least one cut-off router, and preventing each of the remaining routers from communicating with the at least one cut-off router [column 8, lines 59-65],

wherein when a router receives a message from one of the plurality of routers, the router determines if the message is from the at least one cut-off router, and processes the message only when the message is not from the at least one cut-off router [column 9, lines 35-52].

As to claim 27, Rubino et al discloses in a communications system for communications among a plurality of routers controlled by a set of trusted parties in a network having verifiable information identifying at least on functioning router which has become controlled by an untrusted party, a method of operating the network comprising the steps of:

excising the identified router from the network, as discussed above; and

determining whether messages transmitted between the plurality of routers are from the identified router [column 6, lines 36-53].

As to claim 28, Rubino et al discloses the step of reinstating the identified router when a trusted party regains control of the router, as discussed above.

As to claim 29, Rubino et al discloses that the plurality of routers are prevented from communicating with the identified router, as discussed above.

As to claims 30 and 31, Rubino et al discloses that the determining step comprises consulting a data structure representing excised routers to determine if the router is controlled by an untrusted party [column 10, lines 40-54].

As to claim 32, Rubino et al discloses computer executable code stored on a computer readable medium, the code to operate a communications router in a network having a plurality of routers controlled by one or more trusted parties, at least one computer being linked to the

communications router, each of the plurality of routers including a transceiver to transmit and receive messages, the computer executable code comprising:

code to excise from the network a functioning router that has become controlled by an untrusted party , as discussed above;

code to verify that messages transmitted among the plurality of routers are from routers controlled by trusted parties, as discussed above;

code to reinstate an excised router when a trusted party regains control of the excised router, as discussed above.

As to claim 35, Rubino et al discloses a method of excising a router controlled by an untrusted party from an ad-hoc network, the network including a plurality of routers controlled by one or more trusted parties, at least one network control computer communicates with at least one of the plurality of routers, the method comprising the steps of:

determining that a functioning router of the plurality of routers in the network has become controlled by an untrusted party, as discussed above;

excising the router controlled by the untrusted party from the network, as discussed above; and

preventing the plurality of routers from communicating with the router controlled by the untrusted party, as discussed above.

6. Claim 16 is rejected under 35 U.S.C. 102(e) as being anticipated by Haas U.S. Patent No. 6,304,556 B1.

As to claim 16, Haas discloses a mobile communications station which communicates among a plurality of mobile stations controlled by a first of parties in an ad-hoc network in

which stations are arranged in clusters of communication member stations, with one member station in each cluster being a head station for the cluster, each member station communicating with the network through at least on cluster head station, a cluster head station communicating with zero or more cluster head stations, a network linked with the mobile communications station, the mobile communications station comprising:

a transceiver which transmits signals to and receives signals from other mobile stations in the network,

a memory having network information stored thereon [column 7, lines 36-56];

a processor which (i) operates the mobile station as a cluster head or cluster member station [column 8, lines 37-65]; (ii) evaluates an excising signal received from the network control computer, the excising signal indicating that the network control computer has determined that an untrusted party has gained control of a first functioning cluster head or cluster member station and is to be excised from the network; (iii) verifies the authenticity of the excising signal; (iv) excises the first cluster head or cluster member station when the excising signal is authentic; and (v) distributes the excising signal to at least a second cluster head or cluster member station [column 9, lines 32-63].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3, 4, 9 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rubino et al U.S. Patent No. 6,424,629 B1 as applied to claim 1 above, and further in view of Raz et al U.S. Patent No. 6,529,515 B1.

As to claims 3, 9 and 13, Rubino et al does not teach that the electronic processor circuit further causes a message to be transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic.

Raz et al teaches a message to be transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic [column 8, lines 9-27].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al so that a message would have been transmitted to the network control computer and to disregard the excising signal when the excising signal is not authentic.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al by the teaching of Raz et al because it provides efficient use of network resources, without increasing the complexity of application development. Advantageously, it enables the safe execution and rapid deployment of new distributed management applications in a network layer. This active network approach can be gradually integrated into, e.g., an otherwise conventional IP network, and allows smooth migration from conventional IP to programmable networks [column 3, lines 5-15].

As to claim 4, Rubino et al as modified teaches that the electronic processor circuit further evaluates a signal received through the transceiver from another network router. Rubino

et al as modified teaches identifying which network router the signal has been received from [column 15, lines 18-37]. Rubino et al as modified teaches determining if the network router is listed with the information regarding excised routers. Rubino et al as modified teaches discarding the signal when the router is listed. Rubino et al as modified teaches processing the signal when the router is not listed [column 15, lines 39-57].

8. Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rubino et al U.S. Patent No. 6,424,629 B1 as applied to claim 1 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 5 and 14, Rubino et al does not teach that the electronic processor circuit determines the authenticity of the excising signal using a public encryption key.

Schneier teaches the use and benefits of public key encryption [pages 461-462].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al so that the electronic processor circuit would have determined the authenticity of the excising signal using a public encryption key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al by the teaching of Raz et al because public-key is designed to resist chosen-plaintext attacks, their security is based both on the difficulty of deducing the secret key from the public key and the difficulty of deducing the plaintext from the cipher text [page 462].

9. Claims 17-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rubino et al U.S. Patent No. 6,424,629 B1 in view of Chaum U.S. Patent No. 4,947,430.

As to claims 17, 19 and 22, Rubino et al discloses formulating in the control computer an excise signal indicating that an untrusted party has gained control of at least a second functioning router to be excised from the network [column 13, lines 47-63]. Rubino et al discloses adding the information identifying the second router to information regarding excised routers stored in memory of the first router [column 14 line 61 to column 15 line 51]. Rubino et al discloses removing from the first router routing updates corresponding to the second router [column 14 line 61 to column 15 line 51]. Rubino et al discloses removing information corresponding to the second router from a neighbor table of the first router when the second router is listed therein [column 15 line 51 to column 16 line 7]. Rubino et al discloses recomputing a forwarding table in the first router. Rubino et al discloses redistributing the excise signal to each of the plurality of routers, except for the second router [column 15 line 51 to column 16 line 7]. Rubino et al discloses upon receiving a message from another one of the plurality of routers, determining, in each of the plurality of routers an identifier for the router from which the message is received and processing the message only when the information regarding excised routers does not include the identifier authentic [column 16, lines 41-63].

Rubino et al does not teach providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router. Rubino et al does not teach verifying the signature on the excise signal in the first router. Rubino et al does not teach that the digital signature is validated using a public encryption key.

Chaum teaches providing a digital signature of the control computer on the excise signal and transmitting the excise signal to the first router. Chaum teaches verifying the signature on

the excise signal in the first router [column 3, lines 29-42]. Chaum teaches that the digital signature is validated using a public encryption key [column 8, lines 27-46].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al so that a digital signature would have been provided for the control computer. The digital signature would have been verified on the excise signal in the first router. The digital signature would have been validated using a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al by the teaching of Chaum because it requires consent every time the signature is verified and provides a binding signature that cannot be forged to authenticate a user [column 2, lines 36-46].

As to claims 18 and 23, Rubino et al teaches the steps of transmitting a message to the control computer from the first router and causing the first router to disregard the excise signal each when the excise signal is not authentic, as discussed above.

As to claim 20, Rubino et al teaches the step of reinstating the excised second router, as discussed above.

As to claim 21, Rubino et al teaches that a router disregards the message when the information regarding excised routers includes the identifier, as discussed above.

10. Claims 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rubino et al U.S. Patent No. 6,424,629 B1 in view of Wils et al U.S. Patent No. 6,397,260 B1.

As to claims 33 and 34, Rubino et al discloses in a communications system for communications among a plurality of routers controlled by one or more trusted parties in a

network, each of the routers maintaining information regarding functioning routers in the network that have become controlled by untrusted parties, a method of operating a network router comprising the steps of:

receiving a message from one of the plurality of routers in the network , as discussed above;

determining whether the information regarding functioning routers in the network have become controlled by an untrusted party includes the router identifier, as discussed above; and

disregarding the message when the router is listed in the information regarding the message when the routers is listed in the information regarding routers controlled by an untrusted party, as discussed above.

Rubino et al does not teach determining a router identifier for the router that just transmitted the message.

Wils et al teaches determining a router identifier for the router that just transmitted the message [column 3, lines 43-56].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al so that a router identifier would have been included in the transmitted message.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Rubino et al by the teaching of Wils et al because it provides for the automatic transfer of responsibility for forwarding packets to a Backup router, the network manager still bears responsibility for distributing the forwarding load among

multiple routers by configuring different default routers on different hosts. Also, it is necessary to keep the load balanced as network nodes are added and deleted. The process of configuring different default routers can be time consuming, especially on large networks. Also, once an overall load partitioning scheme has been established, the process of manually configuring each node to carry out the scheme is straightforward, and does not generally require the relatively high skill level of a network manager to accomplish [column 6, lines 8-20].

11. Claim 36 is rejected under 35 U.S.C. 103(a) as being unpatentable over Miriyala U.S. Patent No. 6,618,377 B1 as applied to claim 35 above, and further in view of Nessett et al U.S. Patent No. 5,968,176.

As to claim 36, Miriyala does not teach determining step comprises determining a router is controlled by an untrusted party through embedded firewall functionality provided in each of the plurality of routers.

Nessett et al teaches routers with firewall functionality provided in each of the plurality of routers [column 7, lines 48-55].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miriyala so that a compromised router would have been determined through its embedded firewall functionality provided in each of the plurality of routers.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Miriyala by the teaching of Nessett et al because security functions placed in network interface cards, in switches, in routers, and in remote access systems, and provides a system administrator the opportunity to move firewall functionality out to the

variety of devices in the networks to create a pervasive, multilayer firewall. Security features can be distributed in multiple layers to multiple devices, and managed using a coherent security policy management interface that provides a security administrator convenient and clear control over the security properties of the network. The distributed functionality, and convenient and clear control allow scaling advantages for firewalls that now exist only for systems such as distributed remote monitoring dRMON, or other sophisticated network systems that are directed to single purpose functions [column 6, lines 12-26].

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
November 22, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100